PATENT

AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated in the following listing of all claims:

1. (Currently Amended) An information security system comprising:
plural information resources distributed amongst and executable on one or more servers coupled via a communication network to a client entity, the plural information resources having associated trust level requirements, wherein the information security system provides plural trust levels, each of the trust levels corresponding to a respective set of credential types;
a gatekeeper interposed between the client entity and the information resources; and
a credential gathering service common to the plural information resources,
wherein upon receipt of a first request for access to a first of the plural information resources without prior authentication to a sufficient trust level, the gatekeeper redirects the first request to the common credential gathering service and the common credential gathering service obtains a login credential for the client entity in accordance with a mapping rule establishing a correspondence between the sufficient trust level and the respective set of credential types therefor ~~a set of suitable credential types~~.

2. (Original) An information security system, as recited in claim 1,
wherein the first request without prior authentication includes an initial request for access to the first information resource.

3. (Original) An information security system, as recited in claim 1,
wherein the first request without prior authentication includes a subsequent request for access to the first information resource, the subsequent request for access requiring a higher trust level than an initial access request.

4. (Original) An information security system, as recited in claim 1,
wherein upon receipt of a second request for access to a second of the plural information resources, the second request is serviced without redirection to the credential

gathering service, the second information resource having a trust level requirement no greater than that of the first information resource.

B1

5. (Original) An information security system, as recited in claim 1, wherein the correspondence established by the mapping rule is a function of session environment information.

6. (Original) An information security system, as recited in claim 5, wherein the session environment information includes one or more of connection speed, source domain, HTTP environment information, browser type, authentication type, request method, MIME typing, user agent, referrer identity, date and time.

7. (Currently Amended) A credential gathering service providing a single sign-on for sessions that potentially include access to plural information resources having differing security requirements, the credential gathering service comprising:

an input port configured to receive an access request identifying an initiating client entity;

means for associating a trust level requirement with the access request;

an encoding of correspondence between trust levels and credential types, wherein each of the trust levels corresponds to a respective set of the credential types;

selection logic for selecting in accordance with the encoding, a credential type corresponding to the trust level requirement; and

a credential obtaining interface for requesting and receiving a credential of the selected credential type for the initiating client entity.

8. (Original) A credential gathering service as in claim 7, wherein the credential obtaining interface is with the initiating client entity.

9. (Original) A credential gathering service as in claim 7, wherein the credential obtaining interface is with a credentialing authority.

10. (Original) A credential gathering service as in claim 7,

wherein the credential obtaining interface is with a credentialing device selected from the set of retinal scan device, a voiceprint analysis device, a fingerprint analysis device, and a card reader.

11. (Original) A credential gathering service as in claim 7, further comprising:
an authentication interface for authenticating the received credential.

12. (Original) A credential gathering service as in claim 11,
wherein the authentication interface includes a communications interface to an authentication service with one or more pluggable authentication modules corresponding to the credential types.

13. (Original) A credential gathering service as in claim 7,
wherein the initiating client entity is not initially authenticated to a trust level required by a first of the information resources; and
wherein an attempted access to the first information resource by the initiating client entity is redirected to the credential gathering service with an associated trust level requirement corresponding to that required by the first information resource.

14. (Original) A credential gathering service as in claim 13,
wherein the initiating client entity in not initially authenticated.

15. (Original) A credential gathering service as in claim 7,
wherein the log-on request and associated trust level requirement are supplied by the initiating client entity.

16. (Original) A credential gathering service as in claim 7,
wherein the trust level requirement is supplied by the initiating client entity.

17. (Original) A credential gathering service as in claim 7,
wherein the initiating client entity is one of an application and a user.

18. (Original) A credential gathering service as in claim 7,
wherein the credential types include at least two of passwords, certificates, username/password pairs, one time passwords, biometric indicia, and smart cards.

19. (Original) A credential gathering service as in claim 7,
wherein more than one credential type corresponds to a given trust level.

B1

20. (Original) A credential gathering service as in claim 7,
wherein the correspondence between trust levels and credential types is dynamic and the encoding thereof is updateable.

21. (Original) A credential gathering service as in claim 7,
wherein the set of credential types and corresponding trust levels is dynamic and the encoding thereof is updateable.

22. (Original) The credential gathering service of claim 7, encoded in a machine readable medium as software executable in a networked computing environment to provide the plural information resources with the single sign-on.

23. (Original) The credential gathering service of claim 22, wherein the machine readable medium is selected from the set of a disk, tape or other magnetic, optical, or electronic storage medium and a network, wired, wireless or other communications medium.

24. (Currently Amended) A method of providing a single sign-on for plural information resources in an environment that provides plural trust levels, the method comprising:
associating credential types with respective ones of the trust levels;
specifying for each information resource, required ones of the trust levels for accesses thereto;
obtaining at least one credential corresponding to a client entity and authenticating the client entity thereby; and

permitting access to any of the information resources having a specified trust level requirement commensurate with the trust level associated with the authenticated at least one credential.

25. (Original) A method, as recited in claim 36, further comprising:
denying access to any of the information resources having a specified trust level requirement greater than with the trust level associated with the authenticated at least one credential.

B1

26. (Original) A method, as recited in claim 36, further comprising:
for access to any of the information resources having a specified trust level requirement greater than the trust level associated with the authenticated at least one credential, obtaining at least one additional credential corresponding to a client entity and authenticating the client entity thereby;
the at least one additional credential having an associated trust level commensurate with specified trust level requirement.

27. (Original) A method, as recited in claim 36,
wherein the credentials types include at least two of passwords, certificates, username/password pairs, one time passwords, biometric indicia, and smart cards.

28. (Currently Amended) A method of providing sign-on in a networked information environment that provides plural trust levels, the method comprising:
directing a request for access to a first information resource from an insufficiently authenticated client entity to a credential gathering service;
associating a first trust level requirement with the access to the first information resource;
selecting from plural credential types, a credential type having an associated trust level commensurate with the first trust level requirement;
obtaining a credential of the selected credential type for the client entity; and
authenticating the obtained credential.

29. (Original) A method, as recited in claim 28, the method further comprising:

proxying the access request upon successful completion of the authenticating.

30. (Original) A method, as recited in claim 28, the method further comprising:
supplying a cryptographically secured session token to the client entity based on the authenticated credential.

31. (Original) A method, as recited in claim 28, the method further comprising:
after successful completion of the authenticating, proxying a second access request without additional authentication.

32. (Original) A method, as recited in claim 31,
wherein the second access request is directed to the first information resource.

33. (Original) A method, as recited in claim 31,
wherein the second access request is directed to a second information resource, a second trust level requirement associated with access thereto being no greater than the first trust level requirement.

34. (Original) A method, as recited in claim 28,
wherein the associating is by a mapping rule encoded as one or more of a static or dynamic table, a hierarchy of predicates, weighted logic and fuzzy sets.

35. (Original) A method, as recited in claim 28,
wherein the associating is a function of at least resource identifier and environment information.

36. (Currently Amended) A method of providing a security interface common to plural information resources, the method comprising:
associating credential types with trust levels, wherein each of the trust levels correspond to a respective set of the credential types;
specifying for each information resource, a required one of the trust levels for accesses thereto;

with a login service common to the plural information resources, obtaining at least one credential corresponding to a client entity and authenticating an identity of the client entity thereby, wherein the obtained at least one credential is of one of the credential types associated with the required one of the trust levels;

granting or denying access to a first of the information resources based on correspondence between the required trust-level therefor and an authenticated trust level associated with the obtained at least one credential; and

granting or denying access to a second of the information resources based on correspondence between the required trust-level therefor and the authenticated trust level.

37. (Original) A method, as recited in claim 36,

wherein the at least one credential is selected from a set of credential types with associated authentication modules.

38. (Original) A method, as recited in claim 36,

wherein differing trust levels are required for access to the first and second information resources.